Bloquer efficacement les ”fake news” sans connaître leurs réseaux de propagation

Silvia Bonomi, Giovanni Farina, Sébastien Tixeuil

Bloquer efficacement les "fake news" sans connaître leurs réseaux de propagation

Silvia Bonomi[1], Giovanni Farina [1] et Sébastien Tixeuil[2]

[1]*Sapienza Università di Roma, Rome, Italie*
[2]*Sorbonne Université, CNRS, LIP6, F-75005 Paris, France*

Nous considérons un réseau utilisé pour propager des informations. Ce réseau (modélisé à travers un graphe) n'est pas complet et certains nœuds doivent s'appuyer sur des intermédiaires pour communiquer. Cependant, la topologie du réseau est inconnue et un nombre limité de participants malveillants tentent de miner la crédibilité des sources d'information en envoyant de faux messages qui semblent provenir des mêmes sources : des "fake news". Les solutions existantes qui contrecarrent la diffusion de fake news dans ce scénario sont basées sur l'analyse des chemins parcourus par les informations dans le réseau, mais celles-ci peuvent disséminer un nombre factoriel de messages (en la taille du réseau) et nécessiter des calculs complexes aux nœuds pour vérifier l'authenticité de chaque information diffusée. Nous identifions des ensembles de conditions qui permettent une communication fiable entre les nœuds et de complexité optimale, en exploitant une reconstruction partielle de la topologie du réseau.

Mots-clefs : fake news, communication fiable, pannes Byzantines, réseau multi-sauts

1 Introduction

Les "fake news" ont des origines diverses. Nous distinguons les *faits* (la vérité terrain) des *informations* (les octets représentant les vidéos, images, sons, textes, etc.) qui sont produites par une source, des *informations relayées* par un ou plusieurs intermédiaires. Les "fake news" peuvent provenir de sources qui génèrent des informations incorrectes (vis à vis des faits) et de relais malveillants, qui falsifient les informations de la source. L'identification d'informations incorrectes à la source se fait traditionnellement par "fact-checking". Ce travail vise à contrer la falsification d'informations correctes par des relais malveillants.

Plus précisément, nous considérons qu'un réseau de topologie inconnue est utilisé pour propager des informations. Les nœuds de ce réseau souhaitent que leurs messages (contenant une information) parviennent à tous les récipiendaires sans altération. Cependant, des participants malveillants tentent de miner la crédibilité des sources en envoyant des messages falsifiés qui semblent provenir des mêmes sources : des "fake news". Ce problème est connu dans la littérature des systèmes répartis comme le problème de la *communication fiable* (ou diffusion fiable avec une source correcte) et est essentiel pour résoudre des problèmes plus complexes (tels que la diffusion fiable *sans source correcte* ou l'accord réparti). Une solution à la communication fiable garantit l'authenticité, l'intégrité et la livraison des messages échangés au sein du réseau. Il apparaît que ce problème n'est pas toujours résolu efficacement lorsque la topologie du réseau est inconnue. L'une des solutions les plus générales pour obtenir une communication fiable a été fournie par Dolev [Dol81]. Elle garantit l'authenticité et la livraison des messages échangés sur un réseau inconnu dans lequel un nombre limité de participants peuvent se comporter arbitrairement. Cependant, le protocole de Dolev nécessite pour sa mise en œuvre un nombre factoriel (en la taille du réseau) de messages disséminés et un temps de calcul exponentiel à chaque réception d'information, à moins d'envisager des hypothèses supplémentaires à celles nécessaires pour résoudre le problème. Le protocole de Dolev a été récemment amélioré [BFT19] pour certaines familles de topologies, mais sans dépasser ces limites intrinsèques.

Nous proposons un protocole de communication fiable qui, en combinant plusieurs solutions de l'état de l'art, résout de manière optimale le problème de la communication fiable au regard du nombre de messages échangés et de la complexité de la procédure de vérification de l'authenticité des informations.

Nous présentons ici une description informelle de notre protocole et des hypothèses du système qui garantissent son exactitude. Plus de détails sont disponibles dans la version longue de ce travail [BFT20].

2 Modèle

Nous supposons un ensemble fixe de n processus, chacun étant doté d'un identifiant unique. Chaque processus peut échanger des messages avec un sous-ensemble d'autres processus, ses voisins, via les liens de communication. Nous modélisons ces interactions possibles à travers un graphe $G(V,E)$ dans lequel les nœuds sont les processus et les arêtes correspondent aux liens de communication disponibles. On note k la nœud-connexité du graphe (c'est-à-dire le nombre minimum de nœuds qu'il faut supprimer pour déconnecter deux autres nœuds). La topologie du graphe n'est pas connue des processus. Nous considérons deux scénarios alternatifs, `VC` et `VI`, dans lesquels les processus sont conscients (Voisinage Connu) ou non (Voisinage Inconnu) de la composition de leur voisinage. Nous supposons que les messages ne sont pas perdus ou modifiés lors des échanges et qu'un processus ne peut pas mentir sur son identité lorsqu'il s'adresse à l'un de ses voisins (c'est-à-dire que nous supposons que les liens de communication sont fiables et authentifiés). Nous considérons des communications par monodiffusion `CM` (un message envoyé par un processus est reçu par exactement un voisin) ou par diffusion locale `CDL` (un message envoyé par un processus est reçu par tous ses voisins). Nous supposons que dans le système, il ne peut y avoir qu'un nombre limité de processus, au plus f, susceptible d'avoir un comportement arbitraire (voire malveillant). Les autres processus sont corrects, c'est à dire qu'ils exécutent fiablement et honnêtement le code du protocole.

3 Problème de communication fiable

On appelle *source* un processus auteur d'un message qu'il souhaite diffuser aux autres processus d'un réseau. Une solution au problème de la communication fiable garantit l'authenticité, l'intégrité et la livraison des messages échangés entre les processus. Plus précisément, il doit satisfaire les spécifications suivantes.

Communication fiable - spécification du problème :

- *(sûreté)* : si un processus correct délivre un message m, alors m a été envoyé par sa source ;
- *(vivacité)* : si un processus correct envoie un message m, alors m est ultimement délivré par chaque processus correct.

Notons que satisfaire une seule de ses propriétés est trivial : il suffit de ne délivrer aucun message pour satisfaire la sûreté, et de délivrer tous les messages pour satisfaire la vivacité. C'est la satisfaction simultanée de ces deux propriétés qui pose problème.

Dolev a identifié [Dol81] la condition nécessaire et suffisante pour fournir une communication fiable dans un système réparti affecté par au plus f pannes arbitraires. Plus précisément, la nœud-connexité du réseau k doit être supérieure au double des processus fautifs f (c'est-à-dire $k > 2f$). Dolev a proposé une solution algorithmique au problème, mais qui génère un nombre factoriel (en n) de messages au sein du réseau. De plus, une instance du problème NP-Complet *set-packing* doit être résolue par chaque processus pour chaque message reçu. Bien qu'elle ait été récemment améliorée [BFT19] pour certains types de graphes, à ce jour il n'y a pas de solution plus efficace dans le scénario général.

4 Protocole optimal par reconstruction de la topologie

La solution de Dolev [Dol81] au problème de la communication fiable, dénotée `DolevU`, diffuse chaque message par inondation dans le réseau, en collectant les chemins parcourus par les messages.

Dolev a également proposé [Dol81] une solution alternative, dénotée `DolevR`, au problème dans le cas où une partie suffisante de la topologie du réseau serait connue des processus. Ce deuxième protocole nécessite que les messages soient adressés sur des chemins spécifiques du réseau. La connaissance partielle du réseau rend ce protocole optimal en performances, notamment concernant le nombre de messages échangés (linéaire en n) et la complexité de la procédure qui vérifie l'authenticité des messages (linéaire en f). L'exactitude de `DolevR` vient du fait que les processus parviennent toujours à diriger leurs messages sur au moins $f+1$ chemins Disjoints Sans Faute (`DSF`) qui n'ont pas de nœuds communs ni ne passent par des nœuds incorrects.

Nesterenko et Tixeuil [NT09] ont montré qu'une reconstruction partielle de la topologie du réseau est possible malgré la présence de pannes arbitraires dans le système via un protocole appelé `Explorer`.

Cette reconstruction peut toutefois contenir des liens inexistants, et être différente pour chaque processus. Pour cette raison, combiner `Explorer` avec d'autres protocoles n'est pas immédiat et nécessite de prendre en compte ces problèmes.

Nous montrons comment combiner les trois protocoles mentionnés, `DolevU`, `DolevR` et `Explorer`, afin de définir un protocole de communication fiable optimal par rapport au nombre de messages échangés et à la complexité de la procédure de vérification de l'authenticité des messages. On se réfère au protocole obtenu via `CombinedRC`.

Le premier objectif de `CombinedRC` est de permettre aux processus de reconstruire partiellement le réseau, en utilisant `DolevU` et `Explorer`. Plus en détail, chaque processus diffuse la composition de son voisinage à chaque nœud via `DolevU`. Cette procédure a lieu une fois dans le cas de `VC` et chaque fois qu'un nouveau voisin est identifié par un processus dans le cas `VI`. Par la suite, `Explorer` est utilisé par les processus pour calculer la reconstruction en fonction des informations reçues via `DolevU`. Lorsque le réseau est suffisamment reconstruit, chaque couple de processus décide un ensemble de chemins tel qu'au moins $f+1$ satisfont `DSF`. Enfin, chaque paire de processus corrects communique de manière fiable via `DolevR` en utilisant des chemins calculés.

Le point clef concernant l'exactitude de `CombinedRC` dépend de la capacité des processus à identifier $f+1$ chemins satisfaisant `DSF`. Nous identifions des ensembles d'hypothèses permettant aux processus de les calculer au cours de la reconstruction de la topologie partielle. Le détail des résultats et des preuves peut être trouvé dans la version longue de cet article [BFT20].

Théorème 1. *L'hypothèse $k > 3f$ permet à chaque processus correct p_i de calculer $f+1$ chemins `DSF` vers n'importe quel processus correct p_j.*

Théorème 2. *L'hypothèse $k \leq 3f$ n'est pas suffisante pour permettre à tous les processus corrects de calculer $f+1$ chemins `DSF` entre eux.*

Théorème 3. *L'hypothèse $k > 2f + \lfloor f/2 \rfloor$ et au moins une des hypothèses `VC` ou `CDL` permettent à chaque processus correct p_i de calculer $f+1$ chemins `DSF` vers n'importe quel processus correct p_j.*

Conjecture 1. *Les hypothèses $k \leq 2f + \lfloor f/2 \rfloor$, `VC` et `CDL` ne sont pas suffisantes pour permettre à tous les processus corrects de calculer $f+1$ chemins `DSF` entre eux.*

Esquisse des preuves. Les processus fautifs peuvent compromettre l'exactitude du protocole de deux manières : en masquant la présence de certains liens adjacents (réduisant ainsi la nœud-connexité du réseau reconstruit d'au plus f) et en étant sélectionné (au plus f fois) dans les chemins disjoints par les processus corrects. Dans le cas le plus général (`CM` et `VI`), aucune de ces deux actions n'est limitée, mais la topologie partielle qui connecte les seuls processus corrects est toujours reconstructible. Les hypothèses `VC` et `CDL` ne permettent à un processus malveillant que de cacher les liens adjacents à deux processus malveillants, ce qui peuvent réduire la connexité du réseau d'au plus $\lfloor f/2 \rfloor$. Jusqu'à f processus fautifs peuvent toujours être sélectionnés lors du calcul des chemins disjoints par les processus corrects, ce qui suggère que une valeur de nœud-connexité supérieure à $2f + \lfloor f/2 \rfloor$ une borne inférieure pour assurer l'exactitude du protocole. Cependant, l'impossibilité de toujours sélectionner $f+1$ chemins `DSF` dans ce dernier scenario n'est pas prouvée.

5 Analyse de protocole

Une fois l'initialisation effectuée, la complexité du protocole `CombinedRC` pour diffuser un message à partir d'une source fiable est la même que celle de `DolevR`. En détail, `CombinedRC` résout le problème de la communication fiable avec un nombre linéaire de messages dans la taille n du système. En fait, il diffuse les messages via des chemins disjoints. La complexité de la procédure de vérification de l'authenticité des messages est linéaire par rapport au nombre maximal f des pannes, car les processus doivent compter le nombre de copies reçues sur les chemins prédéterminés. La complexité du protocole est donc optimale pour les métriques considérées [BFT20]. `CombinedRC` nécessite une phase d'initialisation pour reconstruire partiellement la topologie. Cette phase demande un certain nombre d'instances de communication fiables de complexité non optimale, `DolevU`. Le nombre de ces instances dépend des hypothèses considérées. En particulier, dans le cas de `VC` et `CDL` il croît linéairement par rapport à la taille n du système et de manière

quadratique dans tous les autres cas. Nos résultats sont résumés dans le tableau 1. Il faut noter que, bien que `CombinedRC` nécessite des hypothèses supplémentaires à celles nécessaires pour résoudre le problème, il permet une communication fiable de manière optimale après une phase d'initialisation qui nécessite un nombre polynomial d'instances de communication fiable non-optimales. L'alternative actuellement disponible dans les mêmes scénarios identifiés dans les théorèmes 1 et 3 est de résoudre le problème toujours de manière inefficace via `DolevU`.

	$k \leq 2f + \lfloor f/2 \rfloor$	$3f \geq k > 2f + \lfloor f/2 \rfloor$	$k > 3f$
`CM + VI`	impossible (?)	impossible	$O(n^2)$
`CM + VC`	impossible (?)	$O(n^2)$	$O(n^2)$
`CDL + VI`	impossible (?)	$O(n^2)$	$O(n^2)$
`CDL + VC`	impossible (?)	$O(n)$	$O(n)$

TABLEAU 1: Nombre d'instances non-optimales de communication fiable requises pour initialiser `CombinedRC`.

6 Conclusion

Nous sommes partis d'un réseau de topologie inconnue utilisé par ses participants pour diffuser des informations, avec l'objectif d'empêcher la propagation d'informations falsifiées générées par un nombre limité de nœuds malveillants. Dans ce scénario, les solutions disponibles pour résoudre le problème de la communication fiable sont coûteuses, nécessitant d'échanger un nombre potentiellement factoriel de messages dans le réseau, et d'exécuter une procédure de vérification d'authenticité qui exige la résolution d'un problème NP-Complet pour chaque message reçu. Nous avons montré comment combiner différents protocoles présents dans la littérature pour obtenir une solution qui, après une phase d'initialisation, résout le problème de manière optimale au regard des métriques considérées.

Il reste un problème ouvert : savoir s'il est possible de fournir une communication fiable de manière efficace, c'est-à-dire avec un nombre de messages qui soit au plus polynomial en fonction de la taille du réseau, ou avec une procédure de vérification de l'authenticité des informations qui soit polynomiale en fonction de la taille du réseau, ou avec ces deux propriétés simultanément, sans considérer d'hypothèses supplémentaires par rapport à celles identifiées par Dolev. Alternativement, il serait intéressant de connaître les conditions minimales pour définir un protocole avec ces caractéristiques de complexité.

Références

[BFT19] Silvia Bonomi, Giovanni Farina, and Sébastien Tixeuil. Multi-hop byzantine reliable broadcast with honest dealer made practical. *J. Braz. Comp. Soc.*, 25(1) :9 :1–9 :23, 2019.

[BFT20] Silvia Bonomi, Giovanni Farina, and Sébastien Tixeuil. Boosting the efficiency of byzantine-tolerant reliable communication. In Stéphane Devismes and Neeraj Mittal, editors, *Stabilization, Safety, and Security of Distributed Systems - 22nd International Symposium, SSS 2020, Austin, TX, USA, November 18-21, 2020, Proceedings*, volume 12514 of *Lecture Notes in Computer Science*, pages 29–44. Springer, 2020.

[Dol81] Danny Dolev. Unanimity in an unknown and unreliable environment. In *22nd Annual Symposium on Foundations of Computer Science, Nashville, Tennessee, USA, 28-30 October 1981*, pages 159–168. IEEE Computer Society, 1981.

[NT09] Mikhail Nesterenko and Sébastien Tixeuil. Discovering network topology in the presence of byzantine faults. *IEEE Trans. Parallel Distributed Syst.*, 20(12) :1777–1789, 2009.